IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Norfolk Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**CRIMINAL NO. 2:12cr184**
	)	
ROBERT PATRICK HOFFMAN II	)	

PROTECTIVE ORDER REGARDING CLASSIFIED INFORMATION

This matter comes before the Court upon the motion of the United States for a Protective Order to prevent the unauthorized disclosure or dissemination of classified national security information and documents, that will be reviewed or made available to the defendant and defense counsel by the government during the prosecution of this case.

Pursuant to the authority granted under Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. III (2006)("CIPA"); the Security Procedures established pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA § 9)("Security Procedures"); Federal Rules of Criminal Procedure 16(d)(1) and 57; the general supervisory authority of the Court, and in order to protect the national security,

IT IS HEREBY ORDERED:

1. The Court finds this case will involve classified national security information. The storage, handling and control of this information will require special security precautions mandated by statute, executive order, and regulation, and access to which requires the

appropriate security clearances, special access, and need-to-know. The purpose of this Protective Order ("Order") is to establish procedures that must be followed by counsel, Court personnel, and any other parties who receive access to classified information or documents in connection with this case.

2. The procedures set forth in this Order, CIPA and the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801, *et seq.*, ("FISA"), will apply to all pretrial, trial, post-trial and appellate matters concerning classified information and may be modified from time to time by further order of the Court acting pursuant to Rule 16(d) of the Federal Rules of Criminal Procedure, sections 3 and 9 of CIPA, FISA, and the Court's inherent supervisory authority to ensure a fair and expeditious trial.

3. Definitions. The following definitions shall apply to this Order:

a. "Classified information" shall mean:

i. Any document or information that has been classified by any Executive Branch agency in the interests of national security or pursuant to Executive Order 13526 or its predecessor Orders, as "CONFIDENTIAL," "SECRET," "TOP SECRET," or additionally controlled as a "CONTROLLED ACCESS PROGRAM," or "SENSITIVE COMPARTMENTED INFORMATION" or any information contained in such document;

ii. Information that is derivatively classified. Derivative classification means the incorporating, paraphrasing, restating or generating in new form information that is already classified under Executive Order 13526 or its predecessor Orders;

iii. Any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party, that the defense knows has been derived from a classified United States Government document, information, or material, regardless of whether such document, information, or material has itself subsequently been classified by the government

pursuant to Executive Order 13526 or its predecessor Orders as "CONFIDENTIAL," "SECRET," "TOP SECRET," or additionally controlled as "CONTROLLED ACCESS PROGRAM," or "SENSITIVE COMPARTMENTED INFORMATION;"

iv. Verbal classified information known to the defense counsel to be classified or verbal classified information that the defense has reason to believe is classified;

v. Any document or information that defense counsel have been notified orally or in writing that such document or information contains classified information;

vi. Any information, regardless of place or origin and including "foreign government information" as that term is defined in Executive Order 13526 and its predecessor orders that is known to contain classified information; and

vii. Any information that defense counsel receives as discovery in this case obtained from an agency that is a member of the United States "Intelligence Community" (as defined in Section 3(4) of the National Security Act of 1947, codified at 50 U.S.C. § 401a(4)), other than the FBI, shall be presumed to fall within the meaning of classified information, unless and until the Classified Information Security Officer or an authorized attorney for the Government advises otherwise in writing.

b. "Controlled Access Program" shall indicate a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level because the vulnerability of, or threat of unauthorized disclosure of specific information (including sources, methods, operations, technologies, or relationships) is exceptional, and the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient.

c. "Document," "Information," and "Materials," shall include, but are not limited to:

i. written or printed matter of any kind, formal or informal, including originals, conforming copies, and non-conforming copies (e.g., a copy of an original with an added notation);

ii. papers, correspondence, letters, reports, summaries, memoranda, notes, communications, telexes, cables, telecopies, telegrams, facsimiles, e-mails, text messages, microfilms, reports, photographs, charts, graphs, maps, invoices, accountings, worksheets, bulletins, transcripts, and messages, as well as alterations, amendments, modifications, and changes of any kind to the foregoing; and all recordings of information on magnetic, electronic, digital, or optical media (including but not limited to those on audio tape, video tape, disks, thumb drives, external hard drives, CD-ROMs, and DVD-ROMs), typewriter ribbons, films and all manner of electronic data processing storage; and

iii. information obtained orally.

d. "Access to classified information" means having access to, reviewing, reading, learning, or otherwise coming to know, in any manner, classified information.

e. "Secure area" means a facility meeting the storage, handling, and control standards for Sensitive Compartmented Information, as accredited by authorized officials from the agencies where the Sensitive Compartmented Information/Controlled Access Program information originated, and the Classified Information Security Officer.

4. Information in the public domain is ordinarily not classified. However, if classified information is reported in the press or otherwise enters the public domain, the information does not lose its classified status merely because it is in the public domain. Any

attempt by the defense to have classified information that has been reported in the public domain but which it knows or has reason to believe is classified, confirmed or denied at trial or in any public proceeding in this case shall be governed by CIPA and all provisions of this Order.

5. All classified documents and information contained therein, shall remain classified unless the documents bear a clear indication they have been declassified by the agency or department that originated the document or information contained therein ("originating agency").

6. Classified Information Security Officers - In accordance with the provisions of CIPA and the Security Procedures, this Court designates Jennifer H. Campbell as the Classified Information Security Officer, and Branden M. Forsgren, Christine E. Gunning, Daniel O. Hartenstine, Joan B. Kennedy, Michael P. Macisso, Carli V. Rodriguez-Feo, Maura L. Peterson, Harry J. Rucker, and W. Scooter Slade as alternate Classified Information Security Officers for this case for the purpose of providing security arrangements necessary to protect from unauthorized disclosure any classified information or documents that have been made available to the defendant as a result of his prior employment with the government, or will be made available to the defense in connection with this case. Defense counsel shall seek guidance from the Classified Information Security Officer with regard to appropriate storage, handling, transmittal, and use of classified information.

7. Government Attorneys - The Court has been advised that National Security Division, Counterespionage Section Trial Attorney Heather Schmidt, and Assistant United States Attorneys Robert Krask and Alan Salsbury, and their respective supervisors, have the requisite security clearances allowing them to have access to the classified information and documents that

relate to this case. Any references to Government Attorneys as used in this Order refer only to the attorneys listed in this paragraph.

8. Secure Area of Review - The Classified Information Security Officer shall arrange for and maintain an appropriately approved secure area for the use of defense counsel. The Classified Information Security Officer shall establish procedures to assure the secure area is accessible to defense counsel during business hours and at other times upon reasonable request as approved by the Classified Information Security Officer. The secure area shall contain a separate working area for defense counsel and will be outfitted with any secure office equipment requested by the defense that is reasonably necessary to the preparation of the defense's case. The Classified Information Security Officer, in consultation with defense counsel, shall establish procedures to assure the secure area is maintained and operated in the most efficient manner consistent with the protection of classified information. No documents or material containing classified information may be removed from the secure area unless so authorized by the Classified Information Security Officer. The Classified Information Security Officer shall not reveal to the Government the content of any conversations he or she may hear among the defense, nor reveal the nature of the documents being reviewed or the work being generated. The presence of the Classified Information Security Officer shall not operate to render inapplicable the attorney-client privilege.

9. If it is necessary for the defendant to review or discuss classified matters, or otherwise meet with defense counsel in the secure area, this will only occur in accordance with the requirements of this Order and under appropriate supervision to ensure that the defendant does not escape or attempt to escape; cause physical injury to himself or others; remove, copy,

alter, or destroy classified information; or attempt to circumvent security restrictions by obtaining access to classified information he is not entitled to review.

a. The United States Marshal's Service shall be responsible for transporting the defendant to and from, and monitoring the defendant while he is present in, the secure area. To arrange for the transportation of the defendant to the secure area for the authorized disclosure and discussion of classified matters, defense counsel must provide the Marshal's Service and the Classified Information Security Officer with written notice forty-eight (48) hours prior to the time that defense counsel seek to meet with the defendant in the secure area. A request for a meeting on Monday must be made on or before 4:00 p.m. on the preceding Wednesday.

b. Once inside the secure area, the defendant will be allowed to meet with defense counsel. The secure area will be monitored by the U.S. Marshal's Service for security purposes through closed-circuit television ("CCTV"). The CCTV will allow only for visual monitoring of the defendant and defense counsel and will not include audio. The CCTV video will not be recorded. If a U.S. Marshal's Service employee inadvertently hears any conversation between the defendant and defense counsel, he or she shall not reveal it to the Government or any member of the prosecution team.

10. Protection of Classified Information - The Court finds that to protect the classified information involved in this case, defense counsel and their approved employees and defense witnesses (collectively referred to herein as "the defense"), shall be given access to classified documents and information as required by the Government's discovery obligations and otherwise as necessary to prepare for proceedings in this case once they have: (1) received notice from the

Classified Information Security Officer that they have been granted Top Secret clearance and access to Sensitive Compartmented Information; (2) been granted access by the appropriate government agencies based on a validated need-to know, signed appropriate non-disclosure statements required by the agencies where any relevant Controlled Access Program information originated, and received appropriate indoctrination; and (3) signed the Memorandum of Understanding. The defendant will continue to be held accountable by the non-disclosure agreements and statements he previously signed and will be required to sign the Memorandum of Understanding acknowledging the procedures for handling classified during the preparation of his case. The signed Memorandum of Understanding shall be filed with the Court. The substitution, departure or removal for any reason from this case of counsel for the defense or anyone associated with the defense as an employee or witness or otherwise shall not release that individual from the provisions of this Order, the Memorandum of Understanding, or any additional non-disclosure agreements or statements executed in connection with this Order.

11. Defense counsel shall file originals of the Memorandum of Understanding executed by the defendant, defense counsel, or employees or other personnel engaged by defense counsel to assist in this case with the Court and the Classified Information Security Officer and serve executed originals of such document upon the Government.

12. The defense may not contact any employee of any government intelligence agency without making prior arrangements with the Government Attorneys, unless the defense files a motion with the Court (which may be *ex parte* at the discretion of defense counsel), to authorize such contact, provides the Government notice of such motion, and obtains a Court order authorizing that contact. This is required because the identities of government intelligence

employees may be classified, and formal arrangements may be required to protect the classified information that may be the subject of discussion by the parties.

13. Access to Classified Information - The defendant, defense counsel, and any later cleared employees or witnesses of defense counsel (in accordance with the procedures outlined above) accompanied by defense counsel shall have access to classified information only as follows:

a. All classified information produced by the Government to the defense in discovery or otherwise, and all classified information possessed, created, or maintained by the defense, shall be stored, maintained, and used only in the secure area established by the Classified Information Security Officer. No classified information shall be maintained by the defense in any other place other than the secure area established by the Classified Information Security Officer.

b. The defendant and defense counsel shall have free access to the classified information made available to them collectively in the secure area established by the Classified Information Security Officer and shall be allowed to take notes and prepare documents with respect to those materials, to be maintained in the secure area.

c. No person, including defense counsel, shall copy or reproduce any classified information in any manner or form, except with the approval of the Classified Information Security Officer or in accordance with the procedures established by the Classified Information Security Officer for the operation of the secure area.

d. All documents, or portions thereof, prepared by the defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information, shall be transcribed, recorded, typed, duplicated, copied or otherwise prepared only by persons who have received an appropriate approval for access to classified information specific to this case, and in the secure area on approved word processing equipment, and in accordance with the procedures approved by the Classified Information Security Officer. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, recordings, disks, thumb drives, CDs, DVDs, exhibits, and electronic or digital copies) that do or may contain classified information shall be maintained in the secure area unless and until the Classified Information Security Officer determines those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to the Government Attorneys or any other party without the permission of the defense.

e. The defense shall discuss classified information only within the secure area or in another area authorized by the Classified Information Security Officer, and shall not discuss, or attempt to discuss, classified information over any standard telephone, cellular telephone, the Internet (including text messaging), office intercommunication system or through any other communication method not specifically authorized by the Classified Information Security Officer.

f. The defense shall not disclose, without prior approval of the Court, the contents of any classified documents or information to any person not named in

this Order except the Court, cleared Court personnel, Government Attorneys, and representatives of the agency or department originating the classified information identified by the Classified Information Security Officer as having the appropriate Top Secret clearance, Sensitive Compartmented Information/Controlled Access Program indoctrination, and the need to know. Government Attorneys shall be given an opportunity to be heard in response to any defense request for disclosure of classified information to a person not named in this Order. Any person approved by the Court for disclosure under this paragraph shall be required to obtain a Top Secret and access to Sensitive Compartmented Information, to sign and submit to the Court the Memorandum of Understanding appended to this Order, to sign any nondisclosure statements required by the originating agencies, and to comply with all the terms and conditions of this Order. If preparation of the defense requires that classified information be disclosed to persons not named in this Order then, upon approval by the Court and upon prior notice to the Government, the Classified Information Security Officer shall promptly seek to obtain security clearances for persons identified by the defense.

g. If Government Attorneys advise defense counsel that certain classified information or documents may not be disclosed to the defendant, then defense counsel, and any agents, consultants, and employees of defense counsel, and defense witnesses shall not disclose such information or documents to the defendant without prior concurrence of the Government Attorneys or, absent such concurrence, approval of the Court. The Government Attorneys shall be given an

opportunity to be heard in response to any defense request for disclosure to the defendant of such classified information.

14. Classified Information Procedures Act - Procedures for the public disclosure of classified information by the defense shall be those established in sections 5, 6, and 8 of CIPA. The Court may issue additional protective orders as needed. To facilitate the defense's filing of notices required under section 5 of CIPA, the Classified Information Security Officer shall make arrangements with the appropriate agencies for a determination of the classification level, if any, of materials or information, either within the possession of the defense or about which the defense has knowledge and which the defense intends to use in any way at any pre-trial proceeding, deposition or at trial. Nothing submitted by the defense to the Classified Information Security Officer pursuant to this paragraph shall be made available to the Government Attorneys unless so ordered by the Court, or so designated by the defense. Any and all items that are classified shall be listed in the defendant's CIPA section 5 notice. To the extent that any classified information is the basis of any motion filed by the defense such motion shall be preceded by a CIPA section 5 notice.

15. Filing of Papers by Defendant - Any pleading or other document filed by the defendant shall be filed under seal with the Classified Information Security Officer or a designee and shall be marked, "Filed In Camera and Under Seal with the Classified Information Security Officer or Designee," unless defense counsel has obtained permission from the Classified Information Security Officer, specific to a particular, non-substantive pleading or document (e.g., motions for extensions of time, continuances, scheduling matters, etc.) which does not contain information that is or may be classified or under seal, to file the document not under seal. The

time of physical submission to the Classified Information Security Officer or a designee shall be considered the date and time of filing. All potentially classified filings shall be submitted to the Classified Information Security Officer or a designee no later than 4:00 p.m. At the time of making a physical submission to the Classified Information Security Officer or designee, defense counsel shall file on the public record on the CM/ECF system a notice of filing that notifies the Court that a filing has been made. The notice should contain only the case caption and an unclassified title of the filing. The Classified Information Security Officer shall immediately deliver, under seal, to the Court, and counsel for the United States, any pleading or document to be filed by the defendant that may contain classified information. The Classified Information Security Officer shall also promptly examine the pleading or document and, in consultation with representatives of the appropriate agencies, determine whether the pleading or document contains classified information. If the designated government classification representative determines the pleading or document contains classified information, the Classified Information Security Officer and the designated government classification representative shall ensure the relevant portion of the document, and only that portion, is marked with the appropriate classification marking and remains under seal. All portions of all papers filed by the defendants that do not contain classified information shall be immediately unsealed by the Classified Information Security Officer and placed in the public record.

16. Filing of Papers by the United States - Those portions of pleadings or documents filed by the United States that contain classified information shall be filed under seal with the Court through the Classified Information Security Officer or a designee. Such pleadings and documents shall be marked, "Filed In Camera and Under Seal with the Classified Information

Security Officer" and shall include in the introductory paragraph a statement that the item is being filed under seal pursuant to this Order, but need not be accompanied by a separate motion to seal. The date and time of physical submission to the Classified Information Security Officer or a designee shall be considered the date and time of filing, and should occur no later than 4:00 p.m. The Classified Information Security Officer shall make arrangements for prompt delivery under seal to the Court and defense counsel of any document to be filed by the Government that contains classified information. After counsel for the United States submits a classified filing to the Classified Information Security Officer, counsel for the United States shall file on the public record, in the CM/ECF system, a notice of filing that should contain only the unclassified case caption and title of the filing. Any electronic filing will serve as a record, and as notice to the Court that classified material has been filed.

17. Sealing of Records - The Classified Information Security Officer shall ensure that a separate sealed record for classified materials is maintained for purposes of later proceedings or appeal.

18. Violations of this Order - Any unauthorized disclosure of classified information may constitute a violation of United States criminal laws. In addition, any violation of the terms of this Order shall be brought immediately to the attention of this Court, and may result in a charge of contempt of court and possible referral for criminal prosecution. Any breach of this Order may also result in termination of an individual's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized use, disclosure, retention, or negligent handling of classified documents or information could cause serious damage, and in some cases, exceptionally grave damage to the national security of the United States. Persons

subject to this Order are also advised that such disclosure may be used to the advantage of a foreign nation or against the interests of the United States, regardless of whether the foreign nation is considered a friend or enemy of the United States. This Order is to ensure that those authorized by the Order to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it, or otherwise use the classified information, without prior written authorization from the originating agency and in conformity with this Order.

19. All classified documents and information to which the defense (including the defendant, counsel for the defendant, any later cleared employee of counsel for the defendant, or cleared defense witnesses) have access in this case are now and will remain the property of the United States. Upon demand of the Classified Information Security Officer, these persons shall return to the Classified Information Security Officer, all classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information. The notes, summaries and other documents prepared by the defense that do or may contain classified information shall remain at all times in the custody of the Classified Information Security Officer for the duration of the case. All such notes, summaries and other documents are to be destroyed by the Classified Information Security Officer one year after the judgment in this case is final or at the conclusion of litigation of any motion filed pursuant to 28 U.S.C. § 2255, whichever date is later, in the presence of defense counsel if so requested.

20. Nothing in this Order shall preclude the Government from seeking a further protective order pursuant to CIPA, FISA, Rule 16(d) or other applicable law as to particular

items of discovery material. The Court may amend this Protective Order and/or issue additional protective orders as needed.

21. A copy of this Order shall be issued forthwith to defense counsel who shall be responsible for advising the defendant, any co-counsel, employees of counsel for the defendant, and defense witnesses who need to know of the contents of this Order. Defendant, defense counsel, and any other individuals who will be provided access to the classified information, shall execute the Memorandum of Understanding described in paragraph 10 of this Order and any additional non-disclosure statements required by the agencies where Sensitive Compartmented Information/Controlled Access Program information originated. Counsel for the defendant shall then file executed originals of the Memorandum of Understanding with the Court and the Classified Information Security Officer and serve an executed original upon the United States. The execution and filing of the Memorandum of Understanding is a condition precedent for defendant, defense counsel, or any other person assisting the defense to have access to classified information. The non-disclosure statements are a condition precedent for access to Sensitive Compartmented Information/Controlled Access Program Information.

SO ORDERED this 7th day of February, 2013 at Norfolk, VA.

/s/
Robert G. Doumar
Senior United States District Judge

ROBERT G. DOUMAR
SENIOR UNITED STATES DISTRICT JUDGE